IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

THE PHOENIX COMPANY, INC., **Plaintiff** v. JAVIER CASTRO-BADILLO; ROCK SOLID TECHNOLOGIES, INC., **Defendants.**	**CIVIL NO. 23-1371 (RAM)**

OPINION AND ORDER[1]

RAÚL M. ARIAS-MARXUACH, United States District Judge

Pending before the Court is co-defendant Rock Solid Technologies, Inc.'s ("Rock Solid" or "Defendant") *Motion to Dismiss Amended Complaint* (the "*Motion to Dismiss*"). (Docket No. 28). For the reasons discussed below, the Court hereby **GRANTS** Defendant's *Motion to Dismiss*.

I. FACTUAL AND PROCEDURAL BACKGROUND

On July 17, 2023, Plaintiff The Phoenix Company, Inc. ("Plaintiff" or "Phoenix") filed a lawsuit against Rock Solid and Javier Castro-Badillo ("Castro-Badillo") (collectively "Defendants"). (Docket No. 1). On December 7, 2023, Plaintiff filed an *Amended Complaint* alleging Defendants violated the Defend Trade Secrets Act, 18 U.S.C. § 1836., as well as the Computer Fraud and

[1] Elizabeth VanKammen, a rising 2L at UVA Law, assisted in the preparation of this Opinion and Order.

Abuse Act, 18 U.S.C. § 1830 ("the CFAA"). (Docket No. 19 ¶ 1.1). Phoenix claims Defendants misappropriated a trade secret and accessed its computers and software without authorization. Id.

Phoenix states it is the "designer, programmer, maker, owner, and sole distributor of the municipal accounting software Monet GFS." Id. ¶ 3.1. This software is marketed and offered to "government entities within Puerto Rico, to entities in states of the United States, and to entities in other countries." Id. ¶ 3.6. Phoenix offers municipalities use of the Monet GFS software through a contract outlining the terms of use and containing a confidentiality agreement. Id. That agreement prohibits users from reverse engineering the software or contracting with a third party to do so. Id. ¶¶ 3.7-3.8. The Monet GFS software also had security software designed to prevent unauthorized access to "the Monet GFS software, the database design, and the access codes." Id. ¶ 4.24.

According to the *Amended Complaint*, the municipality of Morovis ("Morovis") hired Plaintiff to provide the Monet GFS software some time before 2017. Id. ¶ 4.11. After the mayor of Morovis changed in 2017, the contract between Morovis and Phoenix was cancelled. Id. ¶ 4.13. Prior to cancelling the contract, Morovis had hired Castro-Badillo as a systems consultant. Id. ¶ 4.14. Castro-Badillo allegedly "at the direction of and on behalf of Rock Solid . . . hacked into the computers . . . and illegally and without authorization accessed the Monet GFS software that was

installed therein." Id. ¶ 4.25. After the contract was cancelled, Phoenix tried but failed to recover possession of its equipment from Morovis. Id. ¶ 4.15. According to Plaintiff's allegations, Morovis hired Rock Solid following the cancellation of the contract because Rock Solid induced them to do so as a result of their having already acquired the Phoenix trade secrets. Id. ¶ 4.13. Plaintiff alleges this would not have been possible without Castro-Badillo and Rock Solid "stealing the Monet GFS software, the database design, and the access codes from Phoenix." Id. ¶¶ 4.13, 4.20.

Plaintiff claims "[a] similar situation occurred in San Lorenzo, a municipality that was [a] client of Phoenix and a user of the Monet GFS software until July 31, 2021." Id. ¶ 4.21. Plaintiff claims the municipality of San Lorenzo hired Castro-Badillo, and he allegedly proceeded to hack into the software in order to "fashion and/or reverse engineer a migration tool to extract all Monet GFS data in the organized and historic format of the database design." Id. ¶¶ 4.22-4.29. Phoenix avers that it did not learn of these acts until "on or about August 23, 2021 when its employees went to pick up the computers at the Municipality of San Lorenzo." Id. ¶ 4.28.

As a result, Phoenix claims it suffered an interruption in service, lost business revenue of at least $3,400,000, and had to spend significant amounts of time investigating and assessing the

breach and consequent damage, which itself was worth more than $10,000. Id. ¶¶ 4.39-4.41.

On January 5, 2024, Rock Solid filed the *Motion to Dismiss*, arguing that Plaintiff has done nothing more than make "vague conjectures that do not rise to the level required to withstand dismissal." (Docket No. 28 at 2). First, Defendant posits that Plaintiff has failed to plead facts alleging it was in possession of a trade secret. Id. Second, Defendant asserts Phoenix failed to allege security measures taken to preserve the trade secret. Id. at 2-3. Third, Rock Solid claims none of the CFAA claims in the *Amended Complaint* apply to it, instead only providing a basis for relief against Castro-Badillo. Id. at 3. Fourth, Rock Solid argues Plaintiff has failed to provide any factual allegations that link Castro-Badillo and Rock Solid. Id. Fifth and finally, Rock Solid contends that the Trade Secret claims are time-barred and the CFAA claims pertaining to Morovis are time-barred. Id.

Plaintiff responded with its *Opposition to Rock Solid's Motion to Dismiss* (the "*Opposition*") on February 16, 2024. (Docket No. 37). Plaintiff argues that: (a) the statute of limitations pertaining to all claims has not expired; (b) it pled sufficient facts to show the presence of a trade secret and reasonable steps taken to protect said trade secret; (c) Rock Solid can be held vicariously liable for Castro-Badillo's actions under the CFAA;

and (d) damages were sufficiently alleged to satisfy the statute. (Docket No. 37 at 2, 5-6, 8-11, 13).

Defendants filed a *Reply to Plaintiff's Opposition to Rock Solid's Motion to Dismiss* (the "*Reply*") on March 11, 2024, reasserting their arguments. (Docket No. 40).

II. LEGAL STANDARD

Fed. R. Civ. P. 12(b)(6) provides for the dismissal of a complaint that "fails to state a claim upon which relief can be granted." Under Rule 12(b)(6), a plaintiff must plead enough facts to state a claim that is "plausible" on its face, and the "[f]actual allegations must be enough to raise a right to relief above the speculative level . . . on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007) (citations omitted). "[A] plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Id. Further, a complaint will not stand if it offers only "naked assertion[s] devoid of further factual enhancements." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (internal quotation marks and citation omitted). To determine whether a complaint has stated a plausible, non-speculative claim for relief, courts must treat non-conclusory factual allegations

as true. *See* Nieto-Vicenty v. Valledor, 984 F. Supp. 2d 17, 20 (D.P.R. 2013) (citations omitted).

III. DISCUSSION

A. Trade Secret

To assert a claim for misappropriation of a trade secret, a plaintiff must adequately plead that "1) the information is a trade secret; 2) the plaintiff took reasonable steps to preserve the secrecy of the information; and 3) the defendant used improper means, in breach of a confidential relationship, to acquire and use the trade secret." Incase Inc. v. Timex Corp., 488 F.3d 46, 52 (1st Cir. 2007) (citing Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1165 (1st Cir. 1994)), *abrogated on different grounds by* Reed Elsevier, Inc. v. Muchnick, 559 U.S. 154, 160 (2010); *see also* 18 U.S.C. § 1839(3) (defining 'trade secret' as information of which the owner has taken "reasonable measures" to keep secret and which "derives independent economic value" from being secret). For a plaintiff to establish a claim under § 1836, such claim must commence no later than three years after the misappropriation is or should have been discovered. 18 U.S.C. § 1836(d).

As discussed below, the Court finds Plaintiff has not alleged sufficient facts to show there was a trade secret and, in any event, Plaintiff's trade secret claims are time-barred.

i. Plaintiff failed to allege facts showing there was a trade secret

Establishing a claim of trade secret misappropriation requires a plaintiff to adequately describe the trade secret, as "[i]t is hornbook law that 'the parties and the court cannot accurately decide the question of whether a trade secret exists without first understanding what precisely is asserted as a secret.'" Sutra, Inc. v. Iceland Exp., ehf, 2008 WL 2705580, at *3 (D. Mass. 2008) (quoting Charles Tait Graves and Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, 5 Nw. J. Tech. & Intell. Prop. 68, 69 (2006)); *see also* Mallet and Co. Inc. v. Lacayo, 16 F.4th 364, 380-81 (3d Cir. 2021) (explaining that "each . . . element[] is predicated on an adequate identification of what the plaintiff contends to be its trade secret"); Porous Media Corp. v. Midland Brake Inc., 187 F.R.D. 598, 600 (D. Minn. 1999) ("Failure to identify the trade secrets with sufficient specificity renders the Court powerless to enforce any trade secret claim."). The First Circuit has interpreted sufficient specificity to mean the plaintiff has "separate[d] the purported trade secrets from the other information . . . that was **known to the trade**." Allstate, 79 F.4th at 197 (quoting TLS Mgmt. & Mktg. Servs., LLC, 966 F.3d 46, 49 (1st Cir. 2020)) (internal quotations and alterations omitted) (emphasis added).

Phoenix has failed to plead sufficient factual allegations making it plausible it was in possession of a trade secret capable of being misappropriated by Defendants. Phoenix's factual allegations do not distinguish between matters of general knowledge in the trade and the particularities that make its software, Monet GFS, a trade secret. Phoenix alleges "[o]ne of the most innovative and distinct aspects of Monet GFS is the data storage design, which stores the information in a very efficient manner." (Docket No. 19 ¶ 3.3). Plaintiff claims the data storage design and the access codes constitute the trade secret that was misappropriated. Id. Phoenix also states that Monet GFS "contains a wide range of modules," including:

> accounting modules of budget, purchase, accounts payable, recurring disbursements, banking conciliation, financial statements, and municipal taxes. It also has income modules of accounts receivable, patents, collections, and IVU-COFIM. Additionally, it has modules for human resources management, payroll accounting and payments, and fixed assets.

Id. ¶ 3.5. **This fails to adequately describe any characteristics of the software that are distinguishable from that which is within the general or special knowledge of persons skilled in the trade.** *See* Allstate, 79 F.4th at 197; TLS Mgmt., 966 F.3d at 49.

Plaintiff fails to allege that an efficient data storage design is unique to its software and is not common among companies that provide similar services, arguing only that the access codes

for each municipality are different and "the software is updated and changes." [2] (Docket No. 37 at 4). As Phoenix itself avers, the Office of the Commissioner of Municipal Affairs selected two software companies, *i.e.*, Rock Solid and another unnamed company, "to provide services to municipalities." (Docket No. 19 ¶¶ 4.10-4.11). This evinces at least three companies—including Phoenix and Rock Solid—were capable of providing "the same type of software and services." (Docket Nos. 19 ¶¶ 4.10-4.11, 28 at 2). Rock Solid argues that Plaintiff's allegations "prove that Rock Solid had already been engaged to provide the same payroll and accounting services provided by Phoenix. So much so that, in fact, Rock Solid had been selected . . . to provide the services to the Municipalities." (Docket No. 28 at 11). Therefore, the Court finds Plaintiff has failed to allege it provided services using trade secrets to which Rock Solid did not have access as a member of the same trade.

Without identifying a feature of its software not known to others in the business of municipal financial service programs, Phoenix's *Amended Complaint* leaves the Court to "sift through technical data to distill out a trade secret." Touchpoint Solutions, Inc., v. Eastman Kodak Co., 345 F. Supp. 2d 23, 28 (D. Mass. 2004). Nor does Plaintiff detail the necessary differences

[2] These factual allegations are made not in the *Amended Complaint* but instead in Plaintiff's *Opposition*, and "new arguments, however, may not be made in reply briefs." United States v. Toth, 33 F.5th 1, 19 (1st Cir. 2022).

in its *Opposition*, stating only that "the database design and access codes **for each municipality is not the same and the software is updated and changes**." (Docket No. 37 at 4-5) (emphasis added). "New arguments, however, may not be made in reply briefs," so these factual allegations fail to help Plaintiff satisfy the pleading requirements. United States v. Toth, 33 F.4th 1, 19 (1st Cir. 2022).

Moreover, although the access codes themselves are secret, they are not a "trade secret." The access codes accompanying the software "provide for the efficient retrieval of stored data in an ideally organized format to support the functionalities necessary for municipal administration." (Docket No. 19 ¶ 3.3). Courts in other circuits have held that passwords enabling access to confidential information are not themselves trade secrets unless they are "the product of any special formula or algorithm that it developed[.]" State Analysis, Inc. v. Am. Fin. Services Assoc., 621 F. Supp. 2d 309, 321 (E.D. Va. 2009); *see also* North Star Media, LLC v. Winogradsky-Sobel, 2011 WL 13220157, at *10 (C.D. Cal. 2011) ("[A] software company's proprietary algorithm for its computer programs may be a trade secret, . . . but the key to the safe where the algorithm is stored is not."). This because, while passwords "clearly have economic value given that they are integral to accessing [plaintiff's] database, they have no *independent*

economic value in the way a formula or a customer list might have." State Analysis, 621 F. Supp. at 321.

Therefore, Phoenix has failed to plead facts in the *Amended Complaint* showing the Monet GFS software, database design, or access codes constitute a trade secret.

ii. Plaintiff had inquiry notice of trade secret misappropriation, time-barring the action

Even if such facts had been adequately alleged, Plaintiff would still fail to assert a trade secret misappropriation claim insofar as it is time-barred. For a plaintiff to establish a claim under 18 U.S.C. § 1836(d), such claim must commence no later than three years "after the date on which the misappropriation with respect to which the action would relate **is discovered** or by the exercise of reasonable diligence **should have been discovered**. For the purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation." 18 U.S.C. § 1836(d).

a. Plaintiff had knowledge of Rock Solid's access to the Morovis equipment containing alleged trade secrets

Where a plaintiff has a written non-disclosure agreement requiring the return of materials containing trade secrets following the termination or expiration of said agreement, but the contracting party fails to comply and subsequently enters into a relationship with a defendant, courts usually find that the

plaintiff obtained inquiry notice of trade secret misappropriation upon the failure to comply.

In RoboticVISIONTech v. ABB, plaintiff's former employee remained in possession of plaintiff-provided laptops and external hard drives containing "confidential and proprietary information." 2024 WL 1299691, at *3 (D. Del. 2024) (internal quotations omitted). The employee was subject to a policy requiring him "to return work-issued laptops and hard drives upon leaving the employ of [plaintiff]." Id. Upon requesting the return of those devices, the former employee failed to comply, and the plaintiff did not retrieve its devices until later. Id. The former employee was subsequently employed by plaintiff's competitor, the defendant in that case. Id. at *4. The district court, considering these facts, reasoned that the former employee's "failure to return those devices until more than two months after he joined [plaintiff's] competitor, following multiple requests from [plaintiff] that he return those devices, was sufficient to put [plaintiff] on inquiry notice that [former employee] may have misappropriated [plaintiff's] trade secrets." Id. Upon acquiring such notice, the court held, the plaintiff had "a duty to conduct a diligent inquiry to allay those suspicions." Id. Since the plaintiff failed to do so, the claim was time-barred. Id. at *3; *see also* Wang v. Palo Alto Networks, Inc., 2014 WL 1410346, at *7 (N.D. Cal. 2014) (holding plaintiff was on inquiry notice when former employee

failed to return documents containing trade secrets in violation of non-disclosure agreement and proceeded to work for a competitor).

Similarly, in Epstein v. C.R. Bard, Inc., 460 F.3d 183, 188 (1st Cir. 2006), the First Circuit held the plaintiff's trade secret misappropriation claims were time-barred. There, the plaintiff, a designer and manufacturer of medical devices, had provided a particular device to the defendant for a period of time subject to a confidentiality agreement. Id. at 186. Later, after the product was allegedly discontinued, the plaintiff inquired as to why his medical device was still available for sale, despite his having stopped supplying the device to the defendant a year prior. Id. The plaintiff failed to commence litigation within three years of these events, which the circuit court found had placed him on inquiry notice. Id. at 188.

Here, following the termination of its contract with Phoenix, the municipality of Morovis entered into a contract with Rock Solid. Id. ¶ 4.13. Although Phoenix's SaaS contract that it signed with Morovis and San Lorenzo does not expressly require the return of its equipment, the contract does describe the ownership rights of the Monet GFS software, providing the municipalities with a limited license to use it and retaining an ownership interest in Phoenix. (Docket No. 19 ¶ 4.23). Additionally, at the time the contract with Morovis was terminated, "Phoenix

unsuccessfully tried to remove the equipment and the servers installed in Morovis to run Monet GFS . . . . **Phoenix repeatedly demanded** that Morovis grant it access to its computers so that it could retrieve its equipment and **Morovis refused.**" Id. ¶ 4.15 (emphasis added). Following the failed attempts to recover its equipment, Phoenix alleges "Morovis kept the equipment **and continued to use the software.**" Id. ¶ 4.16 (emphasis added).

These averments show Phoenix knew Morovis was allegedly impermissibly in possession of confidential information following the termination of the contract in 2017. Given Morovis' new contract with Rock Solid, Plaintiff **should have known that Rock Solid could likely gain access to that information.** As in RoboticVISIONTech, Plaintiff here was aware that the party allegedly in possession of confidential information, Morovis, had entered into a relationship with Rock Solid by which it was put "on inquiry notice that [Defendant] may have misappropriated [plaintiff's] trade secrets." 2024 WL 1299691, at *4; *see also* Wang, 2014 WL 1410346, at *7; Epstein, 460 F.3d at 188. Further underscoring the notice obtained by Plaintiff, Phoenix alleges "Morovis would not have been able to seamlessly change providers without the theft of Phoenix's trade secrets." (Docket No. 19 ¶ 4.19). That allegedly such a seamless transition was achieved, in fact, is sufficient to put Plaintiff on notice at the time of Morovis contracting with Rock Solid 2017. Plaintiff was on inquiry

notice of trade-secret misappropriation in 2017, four years before initiating the present action and Defendant's *Motion to Dismiss* as to these events is **GRANTED** as time-barred.

b. The San Lorenzo trade secret is time-barred

The only date provided in Plaintiff's *Amended Complaint* regarding when it learned about Castro-Badillo's unauthorized access to the Monet GFS source codes is August 23, 2021. (Docket No. 19 ¶ 4.28). According to Plaintiff, it learned about this unauthorized access "when its employees went to pick up the computers from the Municipality of San Lorenzo." Id.

Plaintiff's *Amended Complaint* alleges misappropriation of a trade secret consistently described as the "Monet GFS software, the database design and the access codes." (Docket No. 19 ¶¶ 3.1-3.5, 3.7, 4.17-4.20). Phoenix uses the **same language** to refer to the trade secret that was misappropriated from both Morovis and San Lorenzo. Id. at ¶¶ 4.17 and 4.23. Nothing in the *Amended Complaint* indicates that the information pertaining to each municipality was different. Id. Phoenix's argument in the *Opposition* that "the breaches were different pieces of information" is unavailing, as there are no such statements in the *Amended Complaint*.[3] Since Plaintiff did not distinguish between

[3] Again, "new arguments, however, may not be made in reply briefs." United States v. Toth, 33 F.5th 1, 19 (1st Cir. 2022); *see also* L.P.R.A. 7(c) ("[T]he moving party may file a reply . . . which shall be strictly confined to responding to new matters raised in the objection or opposing memorandum.").

the trade secrets relevant to the events of 2017 and 2021, there is no plausible way to understand the trade secrets to be two separate pieces of misappropriated information.[4] Id. ¶¶ 4.17, 4.23; *see* B&P Littleford, LLC v. Prescott Mach., LLC, 2021 WL 3732313, at *6 (6th Cir. 2021) (interpreting the DTSA as providing "that the repeated misappropriation of a given trade secret forms a single claim, not multiple claims, because a confidential relationship 'once rent' cannot be 'torn anew.' ") (citing Kehoe Component Sales Inc. v. Best Lighting Prod., Inc., 796 F. 3d 576 (6th Cir. 2015)). Also, the alleged misappropriation was done by the same Defendants, *i.e.*, Rock Solid and Castro-Badillo, regarding the same trade secrets in each instance. (Docket No. 19 ¶¶ 4.17, 4.23). Accordingly, Defendant's *Motion to Dismiss* as to the events relating to the municipality of San Lorenzo is also **GRANTED** as time-barred.

B. Computer Fraud

To assert a claim under 18 U.S.C. § 1030, a plaintiff must establish that the defendant:

> (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was

[4] "[A] continuing misappropriation constitutes a single claim of misappropriation," and both the 2017 and 2021 claims are time-barred because they are appropriately considered a single instance of continuing misappropriation. 18 U.S.C. § 1836(d).

> loss to one or more persons during any one-year period at least $5,000 in value.

Philips Med. Sys. P.R., Inc. v. GIS Partners Corp., 203 F. Supp. 3d 221, 230 (D.P.R. 2016) (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009)). Having alleged facts satisfying those elements, a plaintiff may "maintain a civil action against the violator." 18 U.S.C. § 1030(g). A violator of this statute is one who "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage," id. § 1030(a)(5)(B), such damage being "(I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." Id. § 1030(c)(4)(A)(i)(I). "Loss" includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." Id. § 1030(e)(11). Any action under this title must begin "within 2 years of the date of the act complained of or the date of the discovery of the damage." Id. § 1030(g).

i. Plaintiff alleged facts insufficient to pursue liability against Rock Solid on a theory of vicarious liability

Rock Solid argues "Phoenix clearly alleges that Castro-Badillo was the 'violator,' as it was he who purportedly

'physically accessed the computers and servers owned and provided by Phoenix,' in 2017." (Docket No. 28 at 13) (quoting Docket No. 19 ¶¶ 4.13, 4.15, 4.18). According to Rock Solid, "[t]he Amended Complaint fails to plead any legal relationship between Castro Badillo and Rock Solid," and as such, Rock Solid is not adequately alleged to be a fellow violator against whom Phoenix may assert a claim. Id. at 14. Plaintiff contends, however, that the *Amended Complaint* sufficiently stated facts showing "Defendant Castro-Badillo acted on behalf of Rock Solid when he was hacking into Plaintiff's computers . . . and Defendant Castro-Badillo was paid by Defendant Rock Solid to hack into Plaintiff's computers." (Docket No. 37 at 11). Rock Solid argues Plaintiff has failed to allege that it committed the acts prohibited under 18 U.S.C. § 1030 but that Phoenix instead relies on a misapplied theory of vicarious or contributory liability. (Docket No. 28 at 14).

Courts remain divided as to what conduct the CFAA provides liability for. *See* Advanced Micro Devices, Inc. v. Feldstein, 951 F.Supp.2d 212, 217 (D. Mass. 2013). A "broader" interpretation of the CFAA "defines access in terms of agency or use. Thus, wherever an employee breaches a duty of loyalty, or a contractual obligation . . . their authorization to access information stored on an employer's computer terminates." Id. The "narrower" interpretation, however, imposes liability "to address computer hacking activities and not to supplement state misappropriation of

trade secret laws." Id. The **First Circuit follows the broad view.** *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001), *abrogated on other grounds by* Van Buren v. United States, 593 U.S. 374, 384 (2021). Even under this broad interpretation, the Court finds Plaintiff has failed to sufficiently allege facts to establish that Rock Solid is liable under the CFAA.

Cases in which an employer was held vicariously liable for the actions of its employees or agents are confined predominantly to where a former employee of the plaintiff is subsequently employed by the defendant and provides the defendant with trade-secret information. *See* Coll Builders, 2017 WL 4158661, at *7 (plaintiff's former employee accessed plaintiff's computer systems after employment was terminated and shared proprietary information with defendant); EF Cultural Travel, 274 F.3d at 579 (defendant appeared "to rely on information about [plaintiff] to which he was privy only because of his employment there"); United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (former employee induced current employees to disclose confidential information in breach of express company policy).

Plaintiff cites to Coll Builders Supply, Inc. v. Velez, 2017 WL 4158661, at *9 (M.D. Fla. 2017), in support of its proposition that a company may be vicariously liable under the CFAA for the actions of its employee. Coll Builders falls in the category of

"broad" liability under the CFAA, insofar as the actions at issue did not involve hacking but rather a breach of confidentiality. Id. (holding plaintiff adequately alleged defendants were vicariously liable for plaintiff's former employee's actions where said employee was subsequently hired by defendants).

In EF Cultural Travel, the plaintiff had previously employed the defendant. 274 F.3d at 582. After leaving the plaintiff's company, the defendant hired a third-party hacker whose activities allegedly occurred under the advice of the defendant. Id. The defendant himself shared with the hacker proprietary information he had been contractually prohibited from disclosing by a confidentiality agreement with the former employer/plaintiff. Id. at 583. What EF Cultural Travel and the other cases have in common is the breach of some sort of former employer/employee relationship of trust between the violator and the plaintiff and the creation of a new employer/employee relationship between the violator and the defendant.

No such relationship exists in the present instance. Plaintiff does not allege an employer/employee relationship between Defendants Castro-Badillo and Rock Solid. Plaintiff's allegations merely state "at the direction of and on behalf of Rock Solid, Castro-Badillo hacked into the computers that Phoenix had provided to the Municipality of San Lorenzo and illegally and

without authorization accessed the Monet GFS software that was installed therein." (Docket No. 19 ¶ 4.25).

However, cases alleging hacking occurred "at the direction of" other defendants contain many more facts such as showing a former employer-employee relationship between the directing defendant and the plaintiff. *See* EF Cultural Travel, 274 F.3d at 582. In other cases, the facts showed a former employee of the plaintiff was acting at the behest of their new employer, the defendant. *See, e.g.*, EF Cultural Travel, 274 F.3d at 582; Coll Builders, 2017 WL 4158661, at *9; Nosal, 676 F.3d at 856. Here, the only employer-employee relationship alleged is that between Castro-Badillo and the municipalities of Morovis and San Lorenzo. (Docket No. 19 ¶¶ 4.14 and 4.22). There is no allegation that Rock Solid formally employed Castro-Badillo. Finally, the only contractual relationship alleged that imposes a duty of confidentiality is that between Phoenix and the municipalities. (Docket No. 19 ¶¶ 3.7-3.8). Even if Plaintiff could sufficiently allege another type of relationship between the Defendants, these claims would still fail for inadequate pleading of the loss requirement.

ii. Plaintiff failed to allege facts showing loss of at least $5,000

The final element required for a claim under 18 U.S.C. § 1030(g) is a showing of facts making it plausible that Plaintiff

incurred "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Courts require plaintiffs to "plead facts about its alleged damages under the CFAA." HotSpot Therapeutics, Inc. v. Nurix Therapeutics, Inc., 2022 WL 16637988, at *6 (N.D.Cal. 2022) (granting a motion to dismiss where plaintiff merely stated they "suffered actual damages, including but not limited to lost profits") (quoting Metabyte, Inc. v. NVIDIA Corp., 2013 WL 1729808, at *5 (N.D.Cal. 2013)). For example, another court in this district found the loss requirement met when plaintiffs stated they hired a third party to investigate breaches, and to do so that third party "conducted a forensic analysis of these breaches, and had been paid $6,000." GIS, 204 F. Supp. 3d at 229.

In the *Amended Complaint*, Plaintiff alleges it "suffered a loss due to the time it spent investigating the damages caused by the breach and its loss in business, both of which exceed $5,000" and elsewhere "Defendant's hacking of Plaintiff's system caused an

interruption in service which induced several of Plaintiff's customers to cancel their contracts and therefore caused Plaintiff to lose revenue." (Docket No. 19 ¶¶ 4.33, 6.7). These statements amount to no more than threadbare recitations of the statutory definition of loss under 18 U.S.C. § 1030(e)(11) and as such fail to satisfy the final element of a claim under 18 U.S.C. § 1030. Plaintiff makes no factual allegations as to what investigative measures were taken to discover damages caused by the breach, fails to state what damage, if any, was actually caused by the hacking, and simply states there was an "interruption of service" without alleging facts as to what part of its services were interrupted. (Docket No. 19). Accordingly, Rock Solid's *Motion to Dismiss* is **GRANTED** as to the CFAA claims.

IV. CONCLUSION

For the foregoing reasons, Defendant Rock Solid's *Motion to Dismiss Amended Complaint* at Docket No. 28 is **GRANTED.**

IT IS SO ORDERED.

In San Juan, Puerto Rico, this 9th day of August 2024.

s/Raúl M. Arias-Marxuach
UNITED STATES DISTRICT JUDGE